

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-130733

(43)公開日 平成9年(1997)5月16日

(51)Int.Cl. <sup>6</sup>	識別記号	府内整理番号	F I	技術表示箇所
H 04 N 5/91			H 04 N 5/91	P
G 06 F 13/38			G 06 F 13/38	
G 09 C 1/00	6 6 0	7259-5J	G 09 C 1/00	6 6 0 C
G 11 B 20/10		7736-5D	G 11 B 20/10	H
H 04 L 9/10			H 04 L 9/00	6 2 1 Z
審査請求 未請求 請求項の数 2 O L (全 7 頁) 最終頁に統く				

(21)出願番号 特願平7-285573

(22)出願日 平成7年(1995)11月2日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 松下 耕司

香川県高松市古新町8番地の1 松下寿電子工業株式会社内

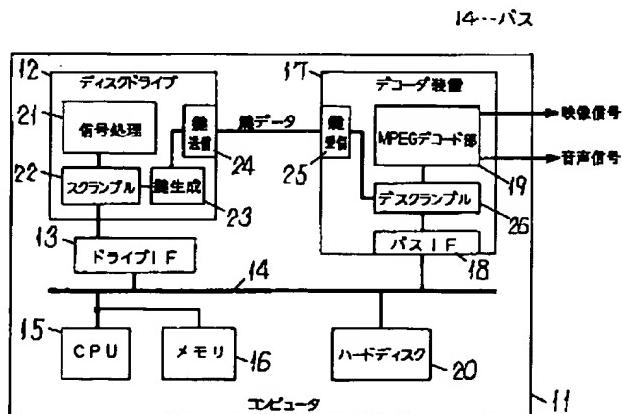
(74)代理人 弁理士 滝本 智之 (外1名)

(54)【発明の名称】 データ再生装置

(57)【要約】

【課題】 コンピュータに接続されたディスクドライブ装置において、記録媒体のディスク上に記録されたデジタル映像音声の著作権を保護するためのデジタルコピーを防止する。

【解決手段】 ディスクからのデジタルデータはディスクドライブ12内のスクランブル回路22で秘匿化されて、コンピュータ11のバス14上を流れ、秘匿化を解く鍵データはバス14とは別の伝送経路を用いてデコード装置17と直接接続される。そして、デコード装置17はバス14上からの秘匿化データをバス14とは別の前記鍵データ用伝送経路から得た鍵データを基にしてデスクランブル回路26にて秘匿化データを解読する構成とする。



## 【特許請求の範囲】

【請求項1】 コンピュータの中央演算装置からの指令に基づいて、記録媒体よりデータ信号を再生する再生手段と、その再生データ信号を秘匿化するための鍵データを発生する鍵データ発生手段と、前記再生データ信号を前記鍵データを用いて秘匿化する秘匿化手段と、その秘匿化された再生データ信号を、前記鍵データに基づいて秘匿解除して出力する秘匿解除手段と、前記秘匿化された再生データ信号を、前記中央演算処理装置からの指令に基づいてデータ転送バスを介して前記秘匿解除手段に転送する転送手段と、鍵データ発生手段により発生された前記鍵データを、前記データ転送バスと異なる伝送経路を介して前記秘匿解除手段に転送する転送手段となるデータ再生装置。

【請求項2】 鍵データ発生手段は、前記中央演算処理装置からの指令に基づいて前記再生データ信号の予め定められた単位ごとに鍵データを変更することを特徴とする請求項1記載のデータ再生装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明はディジタル映像音声信号等のデータ信号が記録された記録媒体より、前記データ信号を再生するデータ再生装置に関するもので、特に、記録媒体から読み出されたデータのパソコンを用いてのコピー防止手段に特徴を有するものである。

## 【0002】

【従来の技術】 近年、MPEG (Moving Pictures Expert Group) などの方式で圧縮されたディジタル映像音声信号をディスクなどの記録媒体に記録し、再生するプレーヤーが用いられるようになってきている。また、同様にディスクドライブをコンピュータ用に用いて、ディジタルデータの記録されたディスクからデータを取りだし、コンピュータの中央演算装置（以下CPUと呼ぶ）で各種のデータが処理できるようになってきている。

【0003】 従来、アナログの映像信号やディジタルの映像信号そのものに関しては、著作権を守る観点からコピー防止の信号を挿入する各種の方式が提案されてはいたが、MPEGなどの方式でディジタル圧縮されたデータが、コンピュータに入った場合、意図的にコピーをしようとすれば、それを防止する手段は存在しなかった。コンピュータで扱うデータはいかに著作権を明示し、そしてコピー防止信号を挿入しようとも、そのデータをコンピュータのCPUで扱うことができる限り、ソフトウェアでコピーおよび書き換え可能である。なぜならば、著作権表示を含めデータを読めるということはデータを転送・コピーできるということであり、コピーしたデータを書き換えるという機能はコンピュータにとって基本的に必要な機能であるので、この基本機能をなくすことはできないからである。したがってコンピュータのソフトウェアで意図的な操作をすれば映画などの著作物につ

いても簡単に、完全なディジタルコピーを作れることになる。

【0004】 以下に従来のデータ再生装置について説明する。図4は従来のデータ再生装置としてコンピュータにCDROMドライブとMPEGデコーダを装着したもののが示すものである。図4において、1はコンピュータ、2はCDROMドライブ、3はCDROMドライブをバスに接続するためのCDROMインターフェース、4はデータを転送するバス、5はコンピュータを制御するCPU、6はデータを一時的に蓄えるメモリ、7はデコーダ装置、8はデコーダ装置をバスに接続するバスインターフェース部、9はMPEG圧縮された映像音声データを伸張するMPEGデコード部、10はハードディスクである。

【0005】 以上のように構成されたデータ再生装置について、以下の動作について説明する。全体はコンピュータの構成をとり、動作はソフトウェアによって与えられCPUによって制御される。CDROMのディスクにはMPEG方式でディジタル圧縮された映像と音声の

データが入っており、これをCDROMドライブ2に装着しコンピュータ1にあるCPU5の制御により圧縮映像音声データがCDROMインターフェース3を介してバス4に読み出される。CPU5はこのデータをいったんメモリ6にバッファとして蓄えた後、データをデコーダ装置7に転送する。実際の動作では、このCDROMドライブ2からメモリ6へのデータ転送とメモリ6からデコーダ装置7へのデータ転送を繰り返すことになる。デコーダ装置7ではバスインターフェース8を介して圧縮されたMPEG映像音声データを受け取り、MPEG

デコード部でディジタル伸張処理をすることによって、映像信号と音声信号にそれぞれ復元され、映像は画面表示され、音声はスピーカから流れる。このような動作により、コンピュータのデータ処理機能を用いてCDROMディスクに記録された圧縮された映像音声データの再生ができる。この場合、CDROMから読み出したデータは、ハードディスク10へ転送することもできる。

## 【0006】

【発明が解決しようとする課題】 しかしながら上記の従来の構成では、MPEGなどの方式でディジタル圧縮された映像音声信号が、コンピュータに入力された場合、通常のコンピュータ用のデータ転送やデータ処理と本質的に差がなく、意図的にコピーをしようとなれば、それを防止することが出来ず、従って、コンピュータのソフトウェアで意図的な操作をすれば映画などの著作物についても簡単に、完全なディジタルコピーを作れるという問題を有していた。

【0007】 本発明は上記従来の問題点を解決するもので、コンピュータのデータ転送・コピーの機能をそのまま生かした状態で、映画などの映像音声ディジタルデータなどはコンピュータの記憶媒体にそのままの形で複製

されないようにし、かつ映像や音声信号のコンピュータ上での再生を可能とするデータ再生装置を提供することを目的とする。

#### 【0008】

【課題を解決するための手段】前記課題を解決するため、本発明のデータ再生装置は記録媒体からの再生データ信号を鍵データを用いて秘匿化し、秘匿化された再生データはコンピュータのデータ転送用バスを用いて転送し、秘匿化を解除する鍵データは前記コンピュータのデータ転送バスとは異なる鍵データ用伝送経路を用いて転送することを特徴としたものである。

【0009】本発明によれば、デジタル映像音声信号は秘匿化された形でコンピュータのデータ転送バス上を流れ、その秘匿化を解く鍵データはコンピュータのデータ転送バス上を通らず、直接、映像音声信号のデコーダ装置へ転送されるので、コンピュータ上での映像音声信号の再生は可能であるが、デジタルコピーは防止することが出来るデータ再生装置を提供出来る。

#### 【0010】

【発明の実施の形態】本発明の請求項1に記載のデータ再生装置は、コンピュータの中央演算装置からの指令に基づいて、記録媒体よりデータ信号を再生する再生手段と、その再生データ信号を秘匿化するための鍵データを発生する鍵データ発生手段と、前記再生データ信号を前記鍵データを用いて秘匿化する秘匿化手段と、その秘匿化された再生データ信号を、前記鍵データに基づいて秘匿解除して出力する秘匿解除手段と、その秘匿化された再生データ信号を、前記中央演算処理装置からの指令に基づいてデータ転送バスを介して前記秘匿解除手段に転送する転送手段と、鍵データ発生手段により発生された前記鍵データを、前記データ転送バスと異なる伝送経路を介して前記秘匿解除手段に転送する転送手段を備えたものであり、記録媒体からの再生データは秘匿化されてコンピュータのデータ転送バス上を流れ、その秘匿化を解除する鍵データはコンピュータの転送バス上と異なる伝送経路を介して、前記秘匿解除手段を含む映像音声のデコーダ装置へ直接転送されるので、コンピュータ上での映像音声信号を再生出来るが、デジタルコピーは防止することが出来る。

【0011】次に、本発明の請求項2に記載されたデータ再生装置は、鍵データ発生手段は、前記中央演算処理装置からの指令に基づいて前記再生データの予め定められた単位ごとに鍵データを変更することを特徴としたものであり、鍵データを頻繁に変更することにより、もし鍵データが盗まれても、解読されるのは限定された秘匿化データのみにとどまるのでデータのスクランブルの安全性を増すことが出来る。

【0012】(実施の形態1) 以下に本発明の請求項1及び請求項2に記載された発明の実施の形態について、図1、図2、図3を用いて説明する。

【0013】図1において、11はコンピュータ、12はディスクドライブ、14はデータを転送するバス、13はディスクドライブをバス14に接続するためのドライブインターフェース、15はコンピュータを制御するCPU、16はデータを一時的に蓄えるメモリ、17はデコーダ装置、18はデコーダ装置をバスに接続するバスインターフェース部、19はMPEG圧縮された映像音声データを伸張するMPEGデコード部、20はハードディスク、21はディスクドライブで読み出したデジタル信号を出力する信号処理部、22はデータを秘匿化するスクランブル部、23は秘匿化のための鍵生成部、24は鍵データ送信部、25は鍵データ受信部、26は秘匿を解除するデスクランブル部である。

【0014】以上のように構成されたデジタル映像音声再生装置について、以下その動作について説明する。全体はやはりコンピュータの構成をとり、その動作はソフトウェアによって与えられCPU15によって制御される。記録媒体であるディスク(図示せず)にはMPEG方式でデジタル圧縮された映像と音声のデータが入っており、これをディスクドライブ12に装着しデータを読み出すと、圧縮されたデジタル映像音声信号はドライブの信号処理部21から出力され、スクランブル部22に入力される。一方鍵生成部23では、ランダムに鍵データが生成され、この鍵データはディスクドライブからのデータ読み出しに連動して、一続きのデータを読み出すたびに鍵データは変更される。スクランブル部22では、この鍵データを用いてスクランブル信号を発生し、それを重畳することにより、ディスクから読み出されたデジタル映像信号を秘匿化する。

【0015】秘匿化されたデータは、CPU15の制御によりドライブインターフェース13を介してバス14に読み出される。CPU15はこのデータをいったんメモリ16にバッファとして蓄えた後、データをデコーダ装置17に転送する。実際の動作では、このディスクドライブ12からメモリ16へのデータ転送とメモリ16からデコーダ装置17へのデータ転送を繰り返すことになる。デコーダ装置17はバスインターフェース18を介して秘匿化されたデータを受け取り、デスクランブル部26へ入力する。

【0016】一方、鍵生成部23で生成された鍵データは鍵送信部24から、バス14とは別経路でデコーダ装置17の鍵受信部25に送信される。この鍵データは頻繁に変更されている上、バス14上を流れず、従って、コンピュータ11のCPU15で鍵データを扱うことが不可能であり、CPU15の処理で秘匿化されたデータのスクランブルを解除することはできない。デスクランブル部26は鍵受信部25で受信した鍵データを用いて、秘匿化データのスクランブルをハードウェアで解除する。スクランブルが解除されたデータは、MPEGデータコード部19でデジタル伸張処理することによつ

て、もともとの映像信号と音声信号にそれぞれ復元され、映像は画面表示され、音声はスピーカから流される。このような動作により、コンピュータのデータ処理機能を用いてディスクから読み出された圧縮された映像音声データを再生することができる。

【0017】図2は、図1におけるディスクドライブ12の鍵データ生成部23、鍵データ送信部24、スクランブル部22を、より詳細に示したブロック図である。図2において、31はドライブ制御マイコン、32は鍵データを生成するランダムデータ発生器、33は鍵データを送信するワンチップマイコン、34はスクランブル信号を生成するランダムデータ発生器、35はスクランブル信号を重畳する排他OR論理回路である。

【0018】以下にその動作を説明する。鍵データの生成はランダムデータ発生器32で行われ、ドライブ制御マイコン31がホストコンピュータ11からのディスクデータの読み出し命令を検知したとき、ランダムに次の鍵データを生成する。このときランダムデータ発生器32は64ビットの鍵データを生成し、それをシリアル信号でワンチップマイコン33とランダムデータ発生器34に伝える。ワンチップマイコン33は鍵データの送信ができるように、外部のデコーダ装置17と相互確認を行い、シリアル通信ポートから鍵データをデコーダ装置17に受け渡すようプログラムされている。またもうひとつランダムデータ発生器34は、受取った64ビットの鍵データを初期値としてランダムデータを発生する。このランダムデータ発生器34は、データ転送命令の後に起きたディスク読み出しのデータ転送タイミングに同期して、16ビット幅のパラレルデータをスクランブル信号として発生させる。ディスクから読み出されたデータはやはり16ビット幅で出てくるので、この両者を排他OR論理回路(16ビット分)35で加算することによりスクランブルされたディスク読み出しデータを得ることができる。

【0019】またディスクのデータが著作権の保護された映画等ではなく、コンピュータの内部で用いる通常のデータの場合はスクランブルをかけないので、その場合はランダムデータ発生器32で生成する64ビットの鍵データは全て0とする。鍵データを0とする指示もドライブ制御マイコン31が、ランダムデータ発生器32に対して行う。このときランダムデータ発生器34で発生するスクランブル信号もすべて0となるので、排他OR論理回路35は入力されたディスク読み出しデータをそのまま出力することになり、スクランブルをかけずに出力することができる。

【0020】ここで注意すべきは、ディスクドライブ12から読み出したデータをデコーダ装置17に転送する際に、ホストコンピュータ11のメモリ16に一続きのデータを蓄えてからデコーダ装置17に転送する動作を繰り返すため、データの発生とデコードの間には時間的

なずれがあることである。このため鍵データを頻繁に変更しようとしても、いつでも変更できることにはならない。図2において説明した方法は、一続きの秘匿化データの転送命令を検知したときのタイミングで鍵データを変更する。このため、その一続きの秘匿化データをコンピュータ11のメモリ16を介してデコーダ装置17に転送するまでの間に、変更された鍵データをデコーダ装置17へ送信することが出来る。このため鍵データの変更と一続きのデータ転送の頭のタイミングを合わせることができ、正しいデスクランブルが可能になる。同時に頻繁な鍵データの変更ができるため、スクランブルの高い安全性が確保される。

【0021】図3は、図1におけるデコーダ装置17の鍵データ受信部25とデスクランブル部26をより詳細に示したブロック図である。図3において、41は鍵データを受信するワンチップマイコン、42はデスクランブル信号を発生するランダムデータ発生器、43はデスクランブルをする排他OR論理回路である。

【0022】以下にその動作を説明する。鍵データの受信にはワンチップマイコン41が用いられ、そのシリアルポートを用いて外部のディスクドライブ12との相互確認を行い、64ビットの鍵データを受信するようにプログラムされている。この64ビットの鍵データはランダムデータ発生器42の初期値として設定される。このランダムデータ発生器42は図2におけるランダムデータ発生器34と同じものである。従ってランダムデータ発生器42ではスクランブル用いたのと同じ16ビット幅のデータ列が、秘匿化データのデータ入力タイミングに同期して発生する。排他OR論理回路43も図2における排他OR論理回路35と同じものである。排他OR論理回路はスクランブル用いたデータ列と同じデータ列を再び加算するとデータがもとに戻る性質があるため、この結果、与えられた鍵データに基づいたデスクランブルが可能になる。デスクランブルされたデータは図1に示すようにMPEGデコード部19の入力信号となる。

【0023】もしもスクランブルされてないデータがバスインターフェース18から入力される場合は、シリアル回線を通じて入力されワンチップマイコン41で受け取って出力する鍵データは全て0である。そのときランダムデータ発生器42で発生するデスクランブル信号も全て0になるので、排他OR論理回路43は入力されたデータをそのまま通し、すなわち、デスクランブル動作をせずにデータを通過させることができる。

【0024】なお、実施例においてスクランブルの手法としてランダムデータ発生器を用いたが、かわりにブロック暗号方式など他の手法を用いてスクランブルしてもよい。また、鍵データの送信にワンチップマイコンを用いたが、これはドライブ制御マイコンで兼ねてもよいし、鍵データ生成部をドライブ制御マイコンの中でソフ

トウェアで実現してもよい。またデコーダ装置17はコンピュータのバスにつなぐ方式としたが、ディスクドライブ12のドライブインターフェース13の部分に接続されていてもよい。

#### 【0025】

【発明の効果】以上のように、本発明のデータ再生装置によれば、コンピュータシステムのデータ転送を用いて映像音声の再生を実現するにあたり、ディスクドライブとデコーダ装置で、それぞれ持っているコンピュータのバスにつながるデータ転送部であるバスインターフェースとは別に、鍵データ入出力部を独立して備え、秘匿化されたデータ自体はバスを通してコンピュータで扱えるが、鍵データはバスとは別に直接接続された経路で伝送されるので、コンピュータのソフトウェアで鍵データを扱うことができない。しかも鍵データが、データ転送中であっても断続的なデータ転送の合間に頻繁に変更されるように構成しておけば、コンピュータ装置のデータ転送・コピー機能をそこなうことなく映像または音声データの複製を防止でき、同時に映像音声の再生表示ができる。また仮に鍵データを何らかの形で知り得たとしても、その鍵データは常時変更されているので解読できるのは限定された範囲の秘匿化データにとどまり、有効に複製の防止ができる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態1におけるデータ再生装置の構成図

【図2】本発明の実施の形態1におけるデータ再生装置の鍵データ生成部と鍵データ送信部とスクランブル部の

#### 詳細なブロック図

【図3】本発明の実施の形態1におけるデータ再生装置の鍵データ受信部とデスクランブル部の詳細なブロック図

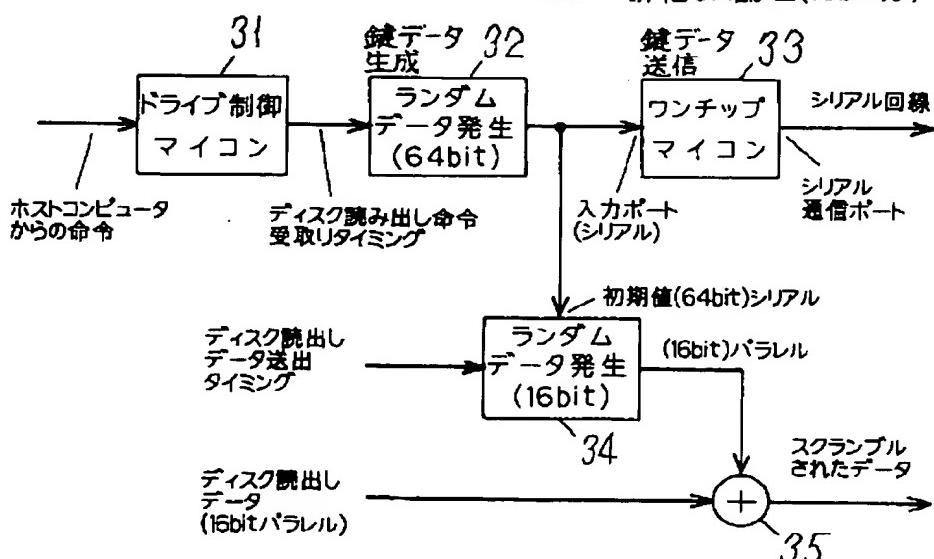
【図4】従来のデータ再生装置のブロック図

#### 【符号の説明】

- |        |                  |
|--------|------------------|
| 1、 11  | コンピュータ           |
| 2      | CD-ROM ドライブ      |
| 4、 14  | バス               |
| 10     | 5、 15 CPU        |
| 6、 16  | メモリ              |
| 7、 17  | デコーダ装置           |
| 8、 18  | バスインターフェース部      |
| 9、 19  | MPEG デコード部       |
| 10、 20 | ハードディスク          |
| 12     | ディスクドライブ         |
| 13     | ドライブインターフェース     |
| 21     | 信号処理部            |
| 22     | スクランブル部          |
| 20     | 23 鍵生成部          |
| 24     | 鍵データ送信部          |
| 25     | 鍵データ受信部          |
| 26     | デスクランブル部         |
| 31     | 32 ドライブ制御マイコン    |
| 32     | ランダムデータ発生(64bit) |
| 33     | ワンチップマイコン        |
| 34     | ランダムデータ発生(16bit) |
| 35     | 排他OR論理回路         |

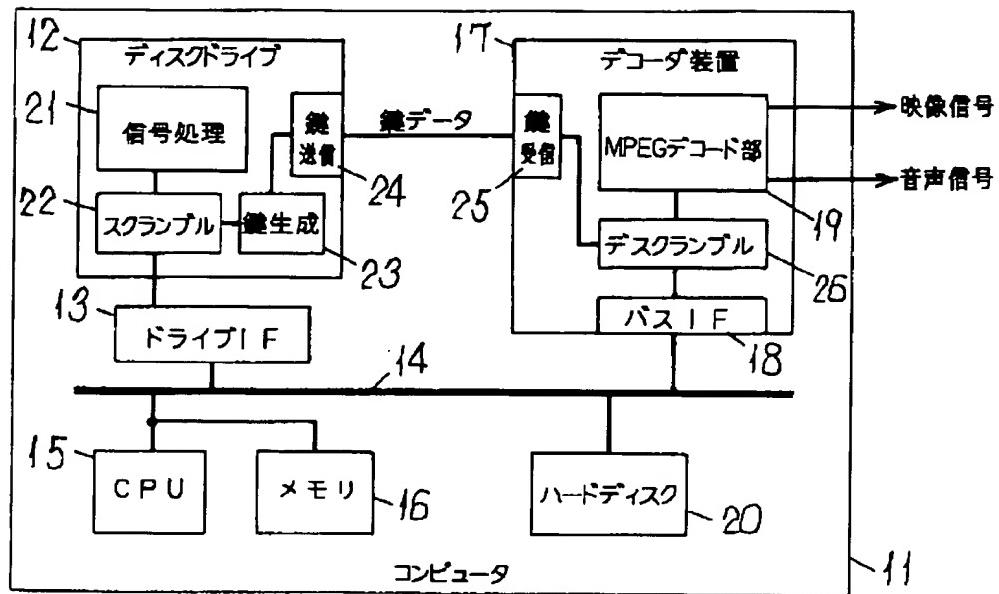
【図2】

#### 35---排他OR論理(16bit分)



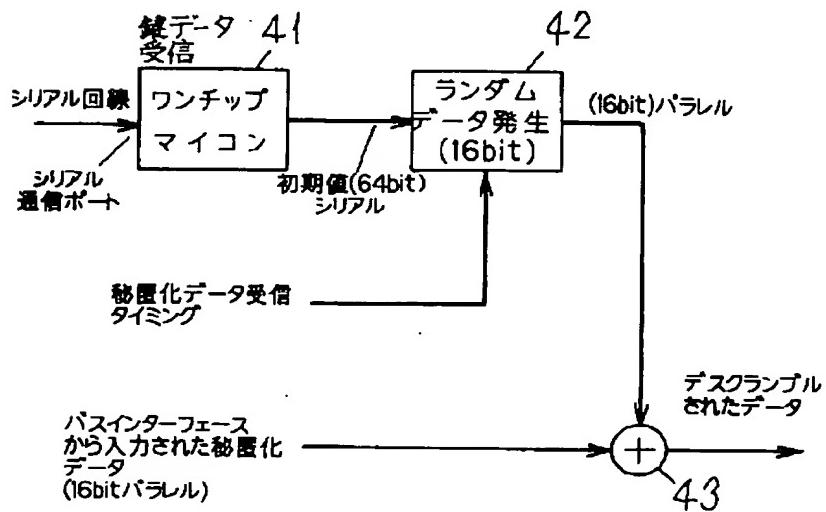
【図1】

14---バス

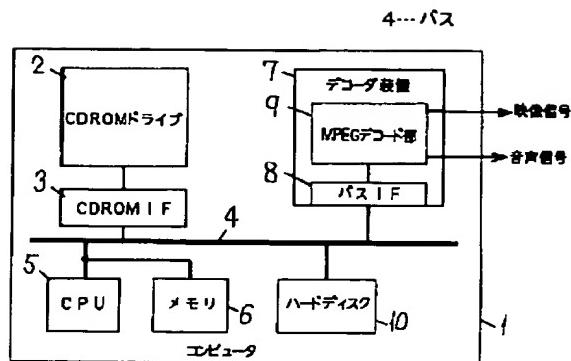


【図3】

43---排他OR論理(16bit分)



【図4】




---

フロントページの続き

(51) Int. Cl. <sup>6</sup>

H 0 4 L 9/12  
H 0 4 N 5/92

識別記号 庁内整理番号

F I  
H 0 4 L 9/00  
H 0 4 N 5/92

技術表示箇所

6 3 1  
H